

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

|                                |            |   |                  |           |
|--------------------------------|------------|---|------------------|-----------|
| Applicants:                    | Rolf Blom  | § | Group Art Unit:  | 2431      |
| Application No                 | 10/597,864 | § | Examiner:        | Zia, Syed |
| Filed:                         | 08/10/2006 | § | Confirmation No: | 7275      |
| Attorney Docket No: P18376-US1 |            | § |                  |           |
| Customer No.: 27045            |            | § |                  |           |

For: KEY MANAGEMENT FOR NETWORK ELEMENTS

**Via EFS-Web**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313.1450

**CERTIFICATE OF TRANSMISSION BY EFS-WEB**

Date of Transmission: \_February 16, 2011

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Jennifer Hardin

\_\_\_\_\_/Jennifer Hardin/\_\_\_\_\_

**APPEAL BRIEF SUBMITTED UNDER 35 U.S.C. §134**

This Appeal Brief is submitted to appeal the decision of the Primary Examiner set forth in a Final Official Action dated September 16, 2010, finally rejecting claims 30-58, and an Advisory Action dated December 13, 2010, maintaining the rejections.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2), and to credit any overpayment, to Deposit Account No. 50-1379.

**Real Party in Interest**

The real party in interest, by assignment, is: Telefonaktiebolaget LM Ericsson (publ)  
SE-164 83  
Stockholm, Sweden

### **Related Appeals and Interferences**

None.

### **Status of Claims**

Claims 1-29 were previously cancelled and are not appealed. Claims 30-58 remain pending, each of which are finally rejected and form the basis for this Appeal.

### **Status of Amendments**

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

### **Summary of Claimed Subject Matter**

| <b>Claim Element</b>  | <b>Specification Reference</b>  |
|---|---|
| <b>30.</b> A method of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of: | Page 5, line 14, <i>et seq.</i><br><br>Figure 3 ; page 14, line 4, <i>et seq.</i> |
| said first cryptographic means generating a freshness token;  | Page 5, line 20, <i>et seq.</i><br>Page 14, line 19, <i>et seq.</i>               |
| said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;  | Page 5, line 22, <i>et seq.</i><br>Page 14, line 22, <i>et seq.</i>               |
| providing said session key (K) to said first network element;   | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |
| providing said freshness token to said second cryptographic means;  | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |
| said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token; and,   | Page 5, line 29, <i>et seq.</i><br><br>Page 15, line 7, <i>et seq.</i>            |
| providing said copy of said session key to said second network element.   | Page 6, line 6, <i>et seq.</i><br>Page 15, line 12, <i>et seq.</i>                |

| <b>Claim Element</b>  | <b>Specification Reference</b>  |
|---|---|
| <b>31.</b> A method of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of: | Page 5, line 14, <i>et seq.</i><br><br>Figure 3 ; page 14, line 4, <i>et seq.</i> |
| said first cryptographic means generating a freshness token;  | Page 5, line 20, <i>et seq.</i><br>Page 14, line 19, <i>et seq.</i>               |
| said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;  | Page 5, line 22, <i>et seq.</i><br>Page 14, line 22, <i>et seq.</i>               |
| providing said session key to said first network element;   | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |
| providing said freshness token to said second cryptographic means;  | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |
| said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token;  | Page 5, line 29, <i>et seq.</i><br><br>Page 15, line 7, <i>et seq.</i>            |
| providing said copy of said session key to said second network element; and,  | Page 6, line 6, <i>et seq.</i><br>Page 15, line 12, <i>et seq.</i>                |
| said first network element and said second network element securely communicating based on said session key and said copy of said session key.  | Page 15, line 15, <i>et seq.</i>  |

| <b>Claim Element</b>   | <b>Specification Reference</b>  |
|--|---|
| <b>42.</b> A system of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises: | Page 5, line 14, <i>et seq.</i><br><br>Figure 3 ; page 14, line 4, <i>et seq.</i> |
| first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;  | Page 5, line 22, <i>et seq.</i><br>Page 14, line 22, <i>et seq.</i>               |
| means for providing said session key from said first cryptographic means to said first   | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |

|  |   |
|--|---|
| network element; and,  |   |
| means for providing said freshness token to said second network domain; wherein said second network domain comprises:                        | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i> |
| second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and, | Page 5, line 29, <i>et seq.</i><br>Page 15, line 7, <i>et seq.</i>  |
| means for providing said copy of said session key from said second cryptographic means to said second network element.                       | Page 6, line 6, <i>et seq.</i><br>Page 15, line 12, <i>et seq.</i>  |

| <b>Claim Element</b>  | <b>Specification Reference</b>  |
|---|---|
| <b>43.</b> A system of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises:  | Page 5, line 14, <i>et seq.</i><br><br>Figure 3 ; page 14, line 4, <i>et seq.</i> |
| first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;   | Page 5, line 22, <i>et seq.</i><br>Page 14, line 22, <i>et seq.</i>               |
| means for providing said session key from said first cryptographic means to said first network element; and,  | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |
| means for providing said freshness token to said second network domain; said second network domain comprises:   | Page 5, line 27, <i>et seq.</i><br>Page 14, line 28, <i>et seq.</i>               |
| second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and,  | Page 5, line 29, <i>et seq.</i><br>Page 15, line 7, <i>et seq.</i>                |
| means for providing said copy of said session key from said second cryptographic means to said second network element, said first network element comprises means for conducting secure communication with said second network element based said session key and said second network element comprises means for conducting secure communication with said first network element based on said copy of said session key. | Page 6, line 6, <i>et seq.</i><br>Page 15, line 12, <i>et seq.</i>                |

The specification references listed above are provided solely to comply with the USPTO's current regulations regarding appeal briefs. The use of such references should not be interpreted to limit the scope of the claims to such references, nor to limit the scope of the claimed invention in any manner.

### **Grounds of Rejection to be Reviewed on Appeal**

- 1.) Whether claims 30-58 are anticipated by Yamaguchi, *et al.* (U.S. Patent No. 5,604,807).

### **Arguments**

#### **1.) CLAIMS 30-58 ARE NOT ANTICIPATED BY YAMAGUCHI**

The Examiner has maintained the rejection of claims 30-58 as being anticipated by Yamaguchi, *et al.* (U.S. Patent No. 5,604,807). The Applicant traverses the rejections.

It must be remembered that anticipation requires that the disclosure of a single piece of prior art reveals every element, or limitation, of a claimed invention. Furthermore, the limitations that must be met by an anticipatory reference are those set forth in each statement of function in a claims limitation, and such a limitation cannot be met by an element in a reference that performs a different function, even though it may be part of a device embodying the same general overall concept. Whereas Yamaguchi fails to teach each and every limitation of claims 30-58, those claims are not anticipated thereby.

Claim 30 recites:

30. A method of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of:  
said first cryptographic means generating a freshness token;  
said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;  
providing said session key (K) to said first network element;

providing **said freshness token** to said second cryptographic means;

said second cryptographic means generating a copy of said session key based on said shared secret key **and said provided freshness token**; and,

providing said copy of said session key to said second network element. (emphasis added)

As presented in claim 30, the Applicant's invention is characterized by the use of a "freshness token" in methods, and systems, for providing secure communication between first and second network elements. A first cryptographic means associated with a first network domain generates a freshness token, and then generates a session key **based on a shared secret key and the generated freshness token**. The session key, which is a function of the freshness token, is then provided to a first network element of the first network domain, and the freshness token is provided to a cryptographic means associated with a second network domain. The second cryptographic means generates a copy of the session key **based on the shared secret key and the received freshness token**, and a copy of the generated session key is then provided to a second network element. The first and second network elements can then communicate securely based on the use of the session key.

In rejecting claim 30 as being anticipated, the Examiner recites the elements thereof and asserts that they are all taught by Yamaguchi, referring to "Fig. 11-13, and col. 10 line 35 to col. 13 line 35." **The undersigned has reviewed the referenced portions of Yamaguchi, however, and can find no teaching of a "freshness token," much less any similar token used in the functions recited in claim 30.** Although Yamaguchi does describe use of a session key, it does not appear that it teaches a session key that is a function of a freshness token.

In responding to those prior arguments, the Examiner asserted in the Final Office Action dated September 16, 2010, that they are not persuasive for the following reasons:

Regarding Claims 1 applicants argued that the cited prior arts (CPA) [Yamaguchi et al. (D. S. Patent No.: 5,604,807)] *"Although Yamaguchi does describe use of a session key, it does not appear that it teaches a session key that is a function of a freshness token. And also does not have no teaching of a freshness token that comprises a random challenge".*

**This is not found persuasive.** The system of cited prior art teaches a system and method that has code gateway between server and network which receives **session key** from key delivery centre and shares it with client. The code communication system consists of multiple server and client connected to a delivery centre through a network. The key delivery centre generates a **session key**. The **session key** is used to establish a session to provide communication between the client and server. Before a session is established, the client outputs a code communication demand to a code gateway. The code gateway first receives the **session key** from the key delivery centre. A first gateway session key delivery section and a second gateway **session key** delivery section delivers this **session key** to the client. The **session key** is decoded in a second encipher-decoder in the code gateway. A **session key** acquisition section receives the **session key** from the code gateway. The received session key is stored in a **session key** holder. A synchronizing establishment unit establishes code synchronisation with the code gateway. A first session establishment section starts a first session with the server. Code synchronization with the server is also performed during this session. A second session establishment unit establishes a second session and a code communication is performed.

As a result, the system of cited prior art does implement and teaches a system and method that relates to inter-network domain key management in communications systems, (Fig.11-13, and col.10 line 35 to col. 13 line 35).

**Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.**

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 30-58 are respectfully maintained. (bold/italic emphasis added)

First, it is noted that the Applicant, in the previously-submitted arguments, identified several **specific** claim elements that are not explicitly, or implicitly, disclosed by Yamaguchi, and that the Examiner's response to those arguments failed to identify those elements in Yamaguchi. For example, the Examiner's responsive argument repeatedly identifies Yamaguchi as teaching a "session key." In that regard, the Applicant agrees. Yamaguchi teaches a "shared session key." (Abstract: "the session key . . . [is] shared at the first and second terminals") Applicant's invention, however, is not *merely* characterized by a "shared session key," but a "shared secret key." Furthermore, according to Applicant's invention, a "session key" is generated by first cryptographic means **based on the shared secret key and a generated freshness token**. Therefore, not only is the "shared session key" disclosed by Yamaguchi not equivalent to the session key employed in Applicant's invention, it is also not analogous to the Applicant's "shared secret key." Moreover, the Examiner has still failed to identify any element in Yamaguchi that can be equated to the Applicant's "freshness token,"

much less the generation of that token by *first* cryptographic means, and the subsequent generation of the session key by *second* cryptographic means **based on the shared secret key and the freshness token**. Accordingly, the Examiner's response to Applicant's arguments fails to point to specific teachings in Yamaguchi of each and every limitation of claim 30 and, therefore, that claim is not anticipated thereby.

### **Examiner's Response to Foregoing Arguments in Advisory Action**

In responding to the foregoing arguments in the Advisory Action dated December 13, 2010, the Examiner focused solely on the statement that: "Although Yamaguchi does describe use of a session key, it does not appear that it teaches a session key that is a function of a freshness token." Based on that statement, the Examiner pointed to a portion of Applicant's specification, wherein it is described how a Key Management Center "generates a freshness token, which could be or include a random **challenge**, a time-stamp and/or a sequence number." (emphasis added) The Examiner then points to a portion of Yamaguchi that describes a random **number** generation unit for generating a session key. (See column 5, lines 60-61); it is noted that the Examiner had not previously raised that teaching of Yamaguchi. Applicant's complete argument, however, is not based merely on a session key being a function of a freshness token, which the Examiner reads as equivalent to a random **number**.

First, a random **challenge** is not equivalent to a random **number**, see arguments *infra* in regard to dependent claim 33. Even if a random **number** is read as equivalent to the claimed "freshness token" in claim 30, Yamaguchi would fail to anticipate the claimed invention. As noted *supra*, a first cryptographic means associated with a first network domain generates a freshness token, and then generates a session key **based on a shared secret key AND the generated freshness token**. **THUS**, the session key, which is a function of the **freshness token AND a shared secret key**, is then provided to a first network element of the first network domain, and the freshness token is provided to a cryptographic means associated with a second network domain. The second cryptographic means generates a copy of the session key **based on the shared secret key AND the received freshness token**, and a copy of the generated



session key is then provided to a second network element. The first and second network elements can then communicate securely based on the use of the session key. The Examiner has not pointed to any teaching in Yamaguchi of generating a session key which is a function of a freshness token AND a shared secret key, even if "freshness token" is read as equivalent to a random number. Therefore, the Examiner's response to Applicant's arguments in the Advisory Action fails to point to specific teachings in Yamaguchi of each and every limitation of claim 30 and, therefore, that claim is not anticipated thereby.

### **Claim 33**

The Applicant further notes that the Examiner's responsive arguments in the Final Office Action and Advisory Action fail to address the additional arguments presented by Applicant with respect to claim 33. In the specific embodiment recited in claim 33, which is dependent from claim 30, the freshness token comprises a random challenge, and the method of claim 30 further comprises the steps of:

said first cryptographic means generating an expected response based on said shared secret key and said random challenge;

providing said expected response to said first network element;

said second cryptographic means generating a response based on said shared secret key and said provided random challenge;

providing said response to said first network element; and,  
said first network element authenticating said second network element based on a comparison between said expected response and said response. (emphasis added)

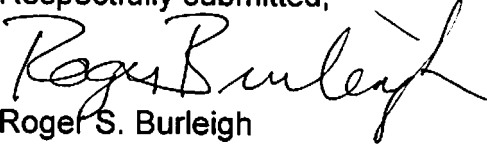
In rejecting claim 33, the Examiner recited the elements thereof and asserted that they are all taught by Yamaguchi, referring to "col. 10 line 35 to col. 11 line 50." The undersigned has reviewed the referenced portion of Yamaguchi, however, and can find no teaching of a freshness token that comprises a random challenge and which is employed in the functions recited in claim 33. Therefore, Yamaguchi also fails to anticipate claim 33.

Whereas independent claims 31, 42, 43, 51 and 55 include limitations analogous to those of independent claim 30 relating to a freshness token, those claims are also not anticipated by Yamaguchi. Similarly, whereas dependent claims 45, 53 and 57 limit the freshness token to a random challenge, further comprising limitations analogous to those of dependent claim 33, they are not anticipated by Yamaguchi. Finally, whereas claims 32 and 34-41 are dependent from claim 30; claims 44 and 46-50 are dependent from claim 42; claims 52 and 54 are dependent from claim 51; and claims 56 and 58 are dependent from claim 55, and include the limitations of there respective base claims, they are also not anticipated by Yamaguchi.

### **CONCLUSION**

The claims currently pending in the application are patentable over the cited prior art, and the Applicant requests that the Examiner's rejections be reversed and the application be remanded for further prosecution.

Respectfully submitted,



Roger S. Burleigh  
Registration No. 40,542  
Ericsson Patent Counsel

Date: February 16, 2011

Ericsson Inc.  
6300 Legacy Drive, M/S EVR1 C-11  
Plano, Texas 75024

(972) 583-5799  
roger.burleigh@ericsson.com

## **CLAIMS APPENDIX**

1-29. (Cancelled)

30. (Previously Presented) A method of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of:

- said first cryptographic means generating a freshness token;
- said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;
- providing said session key (K) to said first network element;
- providing said freshness token to said second cryptographic means;
- said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token; and,
- providing said copy of said session key to said second network element.

31. (Previously Presented) A method of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of:

- said first cryptographic means generating a freshness token;
- said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;
- providing said session key to said first network element;
- providing said freshness token to said second cryptographic means;
- said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token;
- providing said copy of said session key to said second network element; and,

said first network element and said second network element securely communicating based on said session key and said copy of said session key.

32. (Previously Presented) The method according to claim 30, wherein said session key providing step comprises the step of securely providing said session key to said first network element and said session key copy providing step comprises the step of securely providing said copy of said session key to said second network element.

33. (Previously Presented) The method according to claim 30, wherein said freshness token comprises a random challenge and said method further comprises the steps of :

said first cryptographic means generating an expected response based on said shared secret key and said random challenge;

providing said expected response to said first network element;

said second cryptographic means generating a response based on said shared secret key and said provided random challenge;

providing said response to said first network element; and,

said first network element authenticating said second network element based on a comparison between said expected response and said response.

34. (Previously Presented) The method according to claim 33, wherein said first cryptographic means comprises an Authentication and Key Agreement (AKA) algorithm for generating said random challenge, said expected response and said session key, and said second cryptographic means comprises an AKA algorithm for generating said response and said copy of said session key.

35. (Previously Presented) The method according to claim 30, further comprising the steps of:

said first network element providing an identifier associated with said second network domain to said first cryptographic means; and,

said second network element providing an identifier associated with said first network domain to said second cryptographic means.

36. (Previously Presented) The method according to claim 35, wherein said session key and said copy of said session key are generated based on at least one of said identifier associated with said first network domain and said identifier associated with said second network domain.

37. (Previously Presented) The method according to claim 35, further comprising the steps of:

said first cryptographic means identifying said shared secret key based on said identifier associated with said second network domain; and,

said second cryptographic means identifying said shared secret key based on said identifier associated with said first network domain.

38. (Previously Presented) The method according to claim 30, wherein said first cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain and said second cryptographic means is an AAA server provided in a network node of said second network domain.

39. (Previously Presented) The method according to claim 30, wherein said first network domain shares a second secret key with a third network domain comprising third cryptographic means and at least a third network element.

40. (Previously Presented) The method according to claim 30, wherein said first network domain is managed by a first communications network operator and said second network domain is managed by a second different communications network operator.

41. (Previously Presented) The method according to claim 30, further comprising the step of intermittently replacing said shared secret by a new shared secret by basing a key agreement between said first network domain and said second network domain on said shared secret.

42. (Previously Presented) A system of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises:

first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;

means for providing said session key from said first cryptographic means to said first network element; and,

means for providing said freshness token to said second network domain; wherein said second network domain comprises:

second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and,

means for providing said copy of said session key from said second cryptographic means to said second network element.

43. (Previously Presented) A system of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises:

first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;

means for providing said session key from said first cryptographic means to said first network element; and,

means for providing said freshness token to said second network domain;

said second network domain comprises:

second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and,

means for providing said copy of said session key from said second cryptographic means to said second network element, said first network element comprises means for conducting secure communication with said second network element based said session key and said second network element comprises means for conducting secure communication with said first network element based on said copy of said session key.

44. (Previously Presented) The system according to claim 42, wherein said session key providing means is adapted for securely providing said session key from said first cryptographic means to said first network element and said session key copy providing means is adapted for securely providing said copy of said session key from said second cryptographic means to said second network element.

45. (Previously Presented) The system according to claim 42, wherein said freshness token comprises a random challenge and said first cryptographic means comprises means for generating an expected response based on said shared secret key and said random challenge and said second cryptographic means comprises means for generating a response based on said shared secret key and said random challenge, said first network domain comprises means for providing said expected response to said first network element and said second network domain comprises means for providing said response to said first network element, wherein said first network element comprises means for authenticating said second network element based on a comparison between said expected response and said response.

46. (Previously Presented) The system according to claim 45, wherein said first cryptographic means comprises an Authentication and Key Agreement (AKA) algorithm for generating said random challenge, said expected response and said

session key, and said second cryptographic means comprises an AKA algorithm for generating said response and said copy of said session key.

47. (Previously Presented) The system according to claim 42, wherein said first cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain and said second cryptographic means is an AAA server provided in a network node of said second network domain.

48. (Previously Presented) The system according to claim 42, further comprising a third network domain with third cryptographic means and at least a third network element, said first network domain and said third network domain share a second secret key.

49. (Previously Presented) The system according to claim 42, wherein said first network domain is managed by a first communications network operator and said second network domain is managed by a second different communications network operator.

50. (Previously Presented) The system according to claim 42, further comprising means for intermittently replacing said shared secret by a new shared secret, said shared secret replacing means is adapted for replacing said shared secret based on a key agreement between said first network domain and said second network domain using said shared secret.

51. (Previously Presented) A network domain comprising:  
a first network element adapted for communication with a second network element of an external network domain, wherein said network domain and said external network domain sharing a secret key;  
cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;



means for providing said session key from said cryptographic means to said first network element; and,

means for providing said freshness token to said external network domain, wherein said external network domain comprises means for generating a copy of said session key for said second network element based on said shared secret key and said provided freshness token.

52. (Previously Presented) The network domain according to claim 51, wherein said session key providing means is adapted for securely providing said session key from said cryptographic means to said first network element.

53. (Previously Presented) The network domain according to claim 51, wherein said freshness token comprises a random challenge and said cryptographic means comprises means for generating an expected response based on said shared secret key and said random challenge and said external network domain comprises means for generating a response based on said shared secret key and said random challenge, said network domain comprises means for providing said expected response to said first network element and said external network domain comprises means for providing said response to said first network element, wherein said first network element comprises means for authenticating said second network element based on a comparison between said expected response and said response.

54. (Previously Presented) The network domain according to claim 51, wherein said cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain.

55. (Previously Presented) A network domain comprising:  
a first network element adapted for communication with a second network element of an external network domain, wherein said network domain and said external network domain sharing a secret key;

cryptographic means for generating a session key based on said shared secret key and a freshness token provided from said external network domain; and,

means for providing said session key from said cryptographic means to said first network element, wherein said external network domain comprises means for generating said freshness token and for generating a copy of said session key for said second network element based on said shared secret key and said generated freshness token.

56. (Previously Presented) The network domain according to claim 55, wherein said session key providing means is adapted for securely providing said session key from said cryptographic means to said first network element.

57. (Previously Presented) The network domain according to claim 55, wherein said freshness token comprises a random challenge and said cryptographic means comprises means for generating a response based on said shared secret key and said random challenge and said external network domain comprises means for generating an expected response based on said shared secret key and said random challenge and means for providing said expected response to said second network element, said network domain comprises means for providing said response to said second network element, wherein said response and said expected response enables said second network element to authenticate said first network element.

58. (Previously Presented) The network domain according to claim 55, wherein said cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain.

\* \* \*

**EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

None.